# 802.11 for *future* Hotspots & WISPs

APRICOT 2004
KUALA LUMPUR

Matt Peterson

*Bay Area Wireless Users Group*

http://matt.peterson.org/presentations/apricot04/

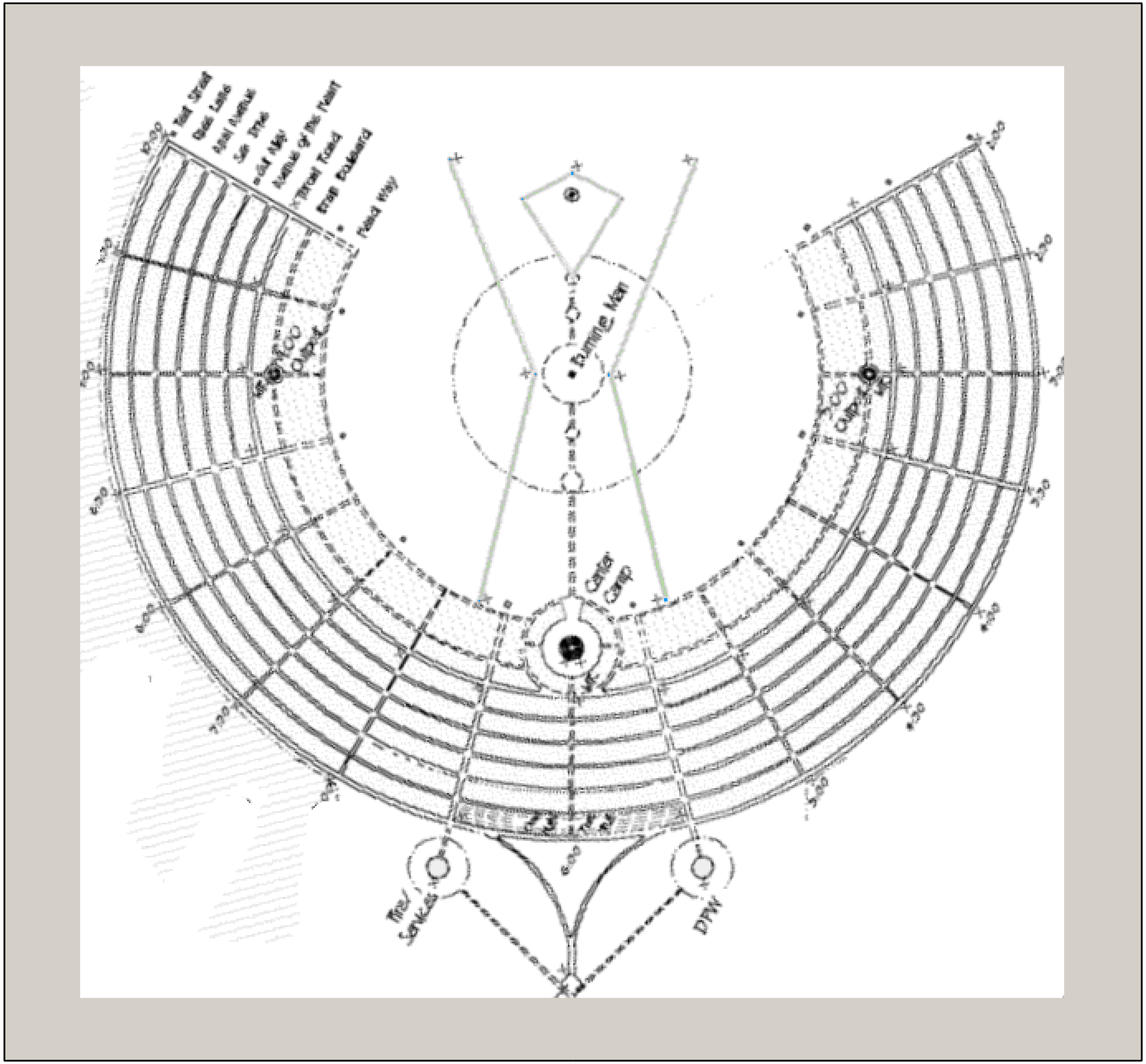
# Today’s Overview

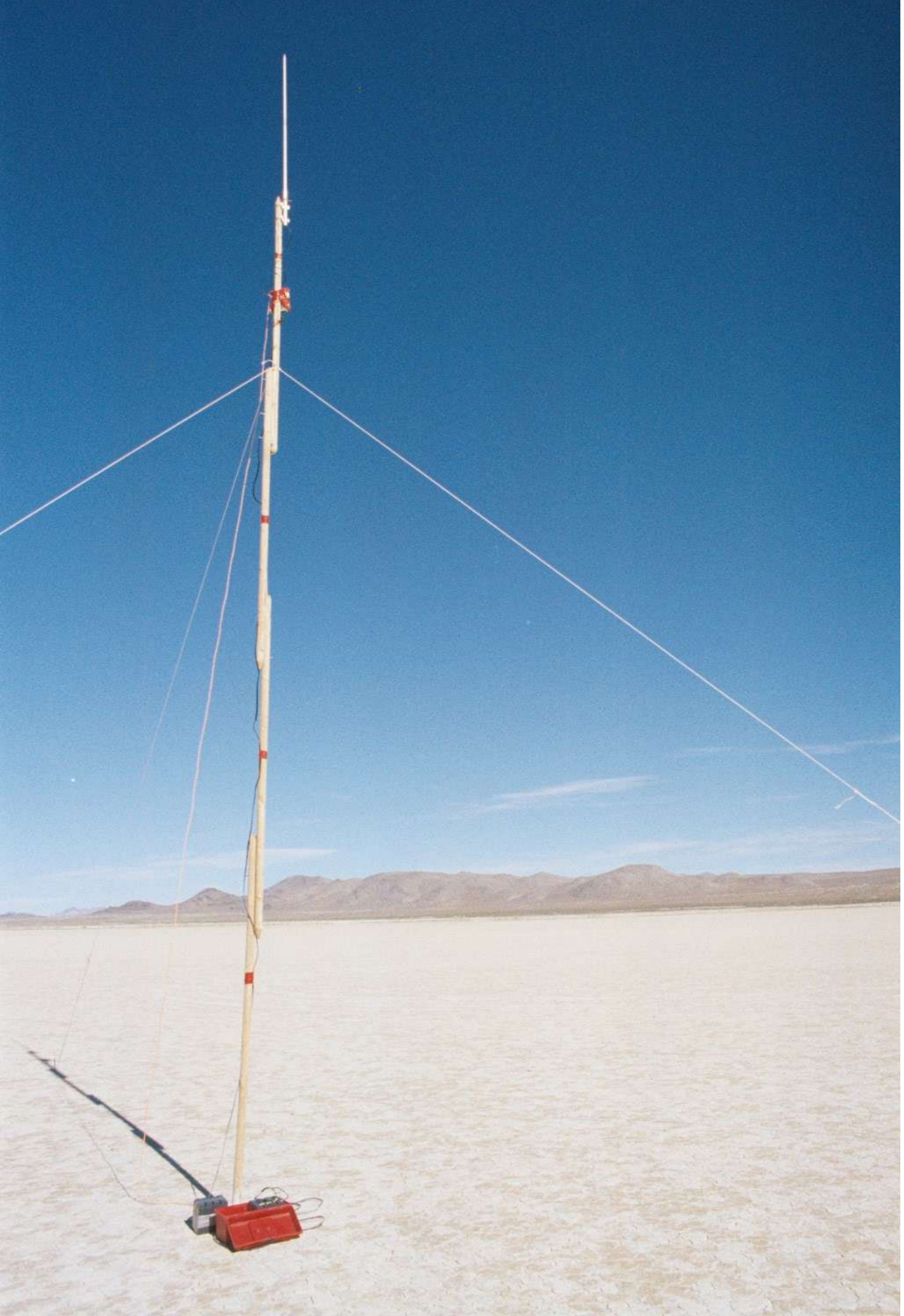
- My 802.11 Resume
- An overview of 802.11 & WLAN concepts
- Industries
  - Hotspot, WISP, Community Wireless
- Knowledge to apply for those “biz models”

# My 802.11 CV

- PlayaNET (co-founder)
  - Intranet for 25k “nomad city” participates @ Burning Man
  - Began with Ricochet (900Mhz 128Kbps proprietary modem), then 802.11, finally 802.11b
  - Provided “phonebook”, scheduling and other communication services

PlayaNET presentation @ http://www.bawug.org/howto/pres/20010816/


10:00
2:00
6:00
Outpost
Outpost
Burning Man
Center Camp
Fire/ Services
DPW

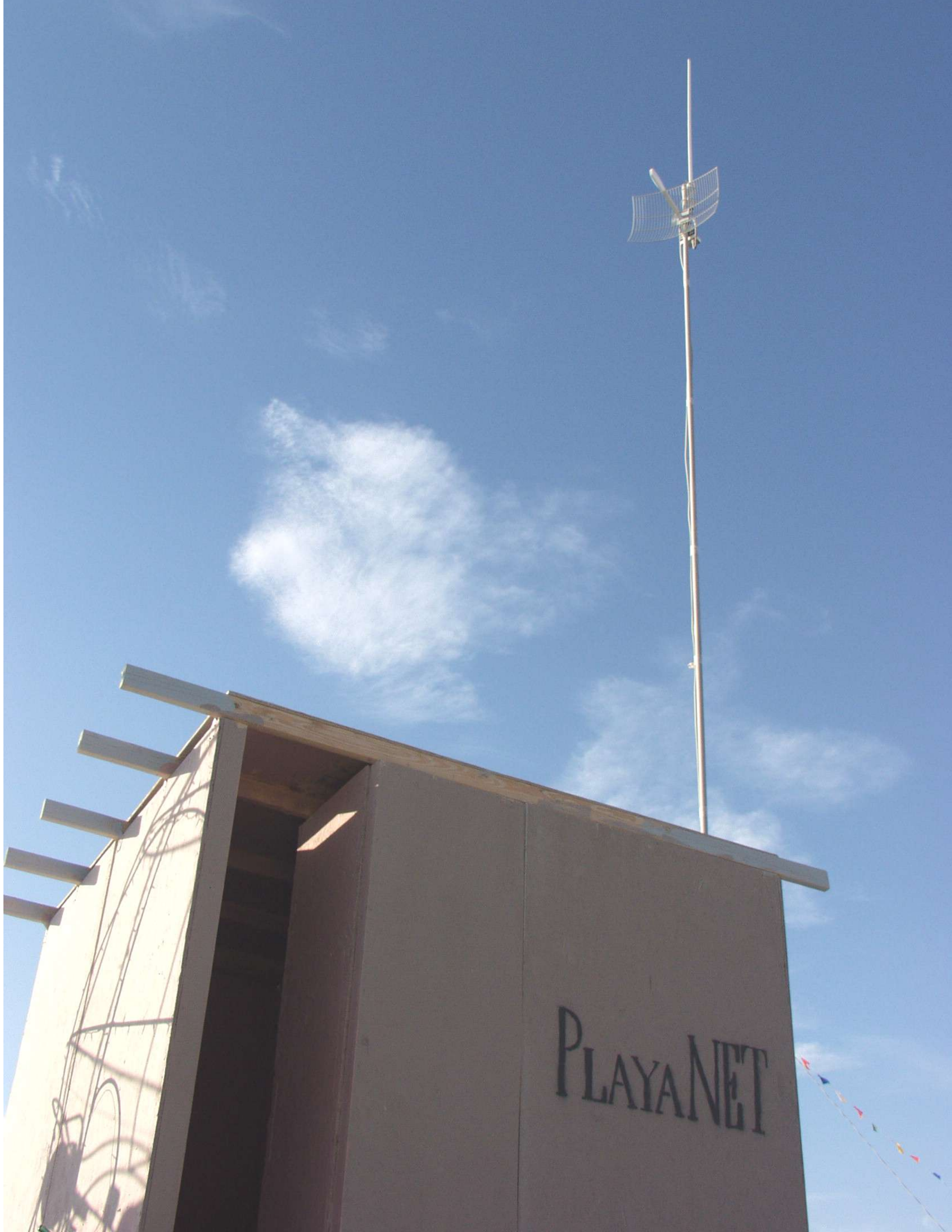


# Test Tower

# Buy professional made towers!

4. PLACE FO
IF YOU WA
PLEASE SEE
THANK
Playa Info
BURNINGMAN
2001
Teled ic
COFF

# Example Kiosk Booth

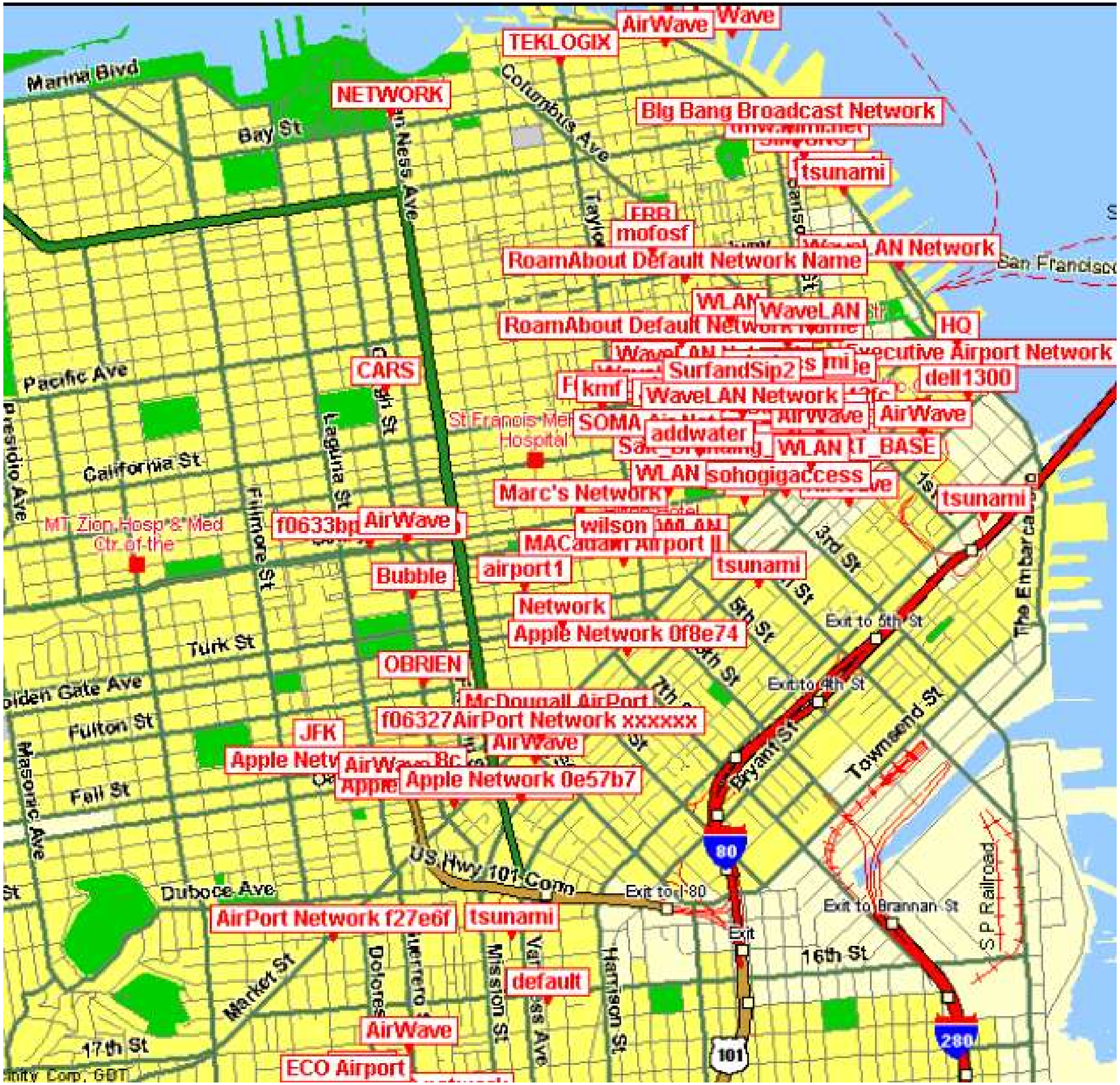


PlayaNET

# My 802.11 CV (cont.)

BAWUG

- Bay Area Wireless Users Group
  - Est. September 2000
  - Founded by IP & RF clued folks to educate
  - Quarterly meeting, active 2k subscriber mailing list
  - Affiliated with worldwide FreeNetworks.org
  - “We don’t build networks”
    - Supply the knowledge, roll your own


AirWave
Wave
TEKLOGIX
NETWORK
Columbus Ave
Big Bang Broadcast Network
tsunami
Marina Blvd
Bay St
Van Ness Ave
Taylor
FBR
mofosf
WaveLAN Network
RoamAbout Default Network Name
San Francisco
WLAN
WaveLAN
RoamAbout Default Network Name
HQ
Executive Airport Network
SurfandSip2
kmf
dell1300
WaveLAN Network
CARS
Pacific Ave
AirWave
AirWave
SOMA
St Francis Mem Hospital
addwater
WLAN
T_BASE
California St
Presidio Ave
Laguna St
WLAN
sohogigaccess
Marc's Network
tsunami
MT Zion Hosp & Med Ctr of the
Fillmore St
f0633bp
AirWave
wilson
MACadam Airport II
tsunami
airport1
Bubble
3rd St
1st
Network
Apple Network 0f8e74
Exit to 5th St
The Embarcadero
Turk St
OBRIEN
Golden Gate Ave
Exit to 4th St
McDougall AirPort
f06327AirPort Network xxxxxx
Fulton St
JFK
AirWave
Townsend St
Bryant St
Masonic Ave
Apple Netw
AirWave
Apple
Apple Network 0e57b7
Fell St
80
US Hwy 101 Conn
Exit to I-80
Duboce Ave
AirPort Network f27e6f
tsunami
Exit to Brannan St
Exit
S P Railroad
16th St
Dolores
Guerrero
Mission St
Van Ness Ave
Harrison St
default
Market St
AirWave
17th St
101
280
ECO Airport

BAWUG

- Milestones
  - Many 1st public talks/releases on
    - 802.1x (Microsoft IETF author)
    - WEP key flaw (UC Berkeley research student)
    - OpenAP (complete Open Source Linux WLAN router)
  - Many past & present company presentations
    - Antennas (Vivato, Swedcom, “Pringles Can”)
    - Mesh (Instant802, UltraDevices)
    - AP routers (Musenki, Soekris, Vernier)
    - etc.

# My 802.11 CV (cont.)

- Independent Consultant

  Surf and Sip™ Network

  - International hotspot firm

  MetroFi

  - National WISP
  - Other small firms

- ***"Authority Figure"***
  - USA Today, Wall St Journal, Wired, TechTV, etc.

# Workshop

- Style
  - No sales pitch :-)
  - Please be interactive, interruptions are welcomed (and encouraged!)
- Not today
  - Bluetooth, HomeRF, HiperLAN, 802.16 “WiMAX”
- What would you like to learn today?
  - Name, country, goals
  - I’ll attempt to “tune” the workshop towards audience

# 802.11 = Wireless Fidelity

Wi Fi®
CERTIFIED

- **WiFi Alliance**
  - Certify interoperability between manufactures products claiming to follow IEEE standards
  - Doesn’t author standards, only recommendations and define their own certification requirements “seal of approval”

http://www.wi-fi.org/

# WiFi / 802.11 Overview

# Why 802.11 Wireless?

- **End-to-end**
  - *eliminate telco/monopoly "partner"*
- **Bandwidth**
  - *own infrastructure, scale as needed*
- **Fast**
  - *anywhere from 0 to ~25Mb/s (real-world throughput)*
- **Unlicensed**
  - *no licensing/bidding, zero to limited recurring cost*
- **Standards**
  - *very economical, mass production, plug-n-play*

- 95% of 2005 laptops will be WiFi-enabled (InStat/MDR)

# Why *not* 802.11 Wireless?

- Typically, we're secondary band users, primary being government; also must accept interference (X10 "spy" cameras, cordless phones, baby monitors)
  - Low power and above interference susacceptable
- Anyone can use it (just like walkie-talkies, ***requires*** some level of coordination for high congested areas)
- Doesn't scale for large deployments (802.11 = **W**ireless **L**ocal **A**rea **N**etwork.. Not WAN)
- Insecure "out of the box"

# IEEE Standards

| IEEE | Speed | Frequency | Ratified |
|---|---|---|---|
| 802.11 | 2Mb/s | 2.4Ghz | 1997 |
| 802.11b | 11Mb/s | | 1999 |
| 802.11g | 54Mb/s | | 2003 |
| 802.11a | | 5.2/5.8Ghz | 1999 |
| 802.11n | 100Mbps | 5Ghz? | 2006? |

Download IEEE 802 specs @ http://standards.ieee.org/getieee802/

# 802 ‘alphabet soup’

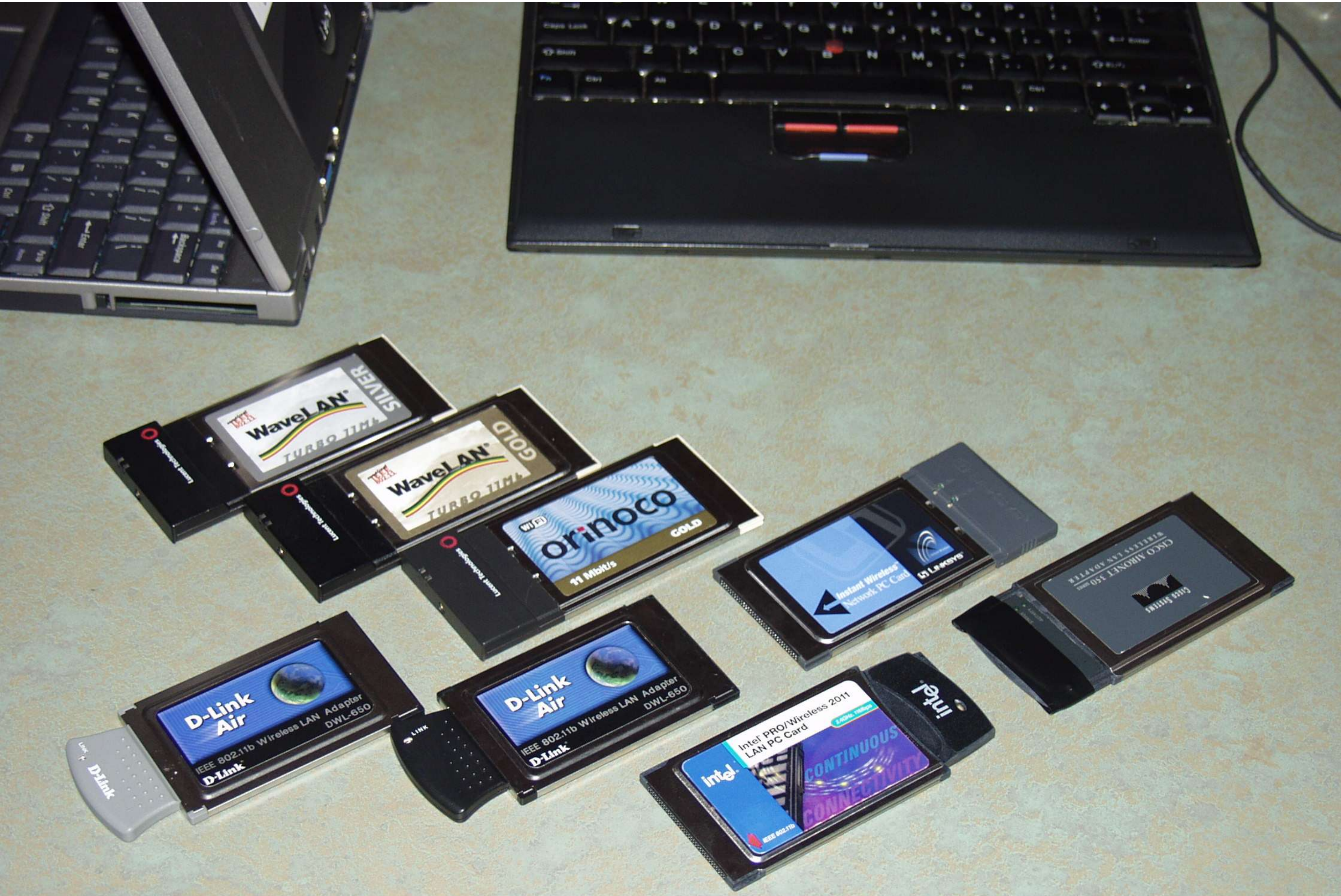
| | |
|---|---|
| 11a | OFDM in “UNI” 5Ghz |
| 11b | CCK in 2.4Ghz |
| 11e | Add QoS into MAC |
| 11f | IAPP, support roaming |
| 11g | OFDM in 2.4Ghz |
| 11h | Dynamic freq. & power adjustment |
| 11i | Strong encryption, dynamic keying |
| 1x | AAA for wired & wireless networks |

# WLAN Concepts

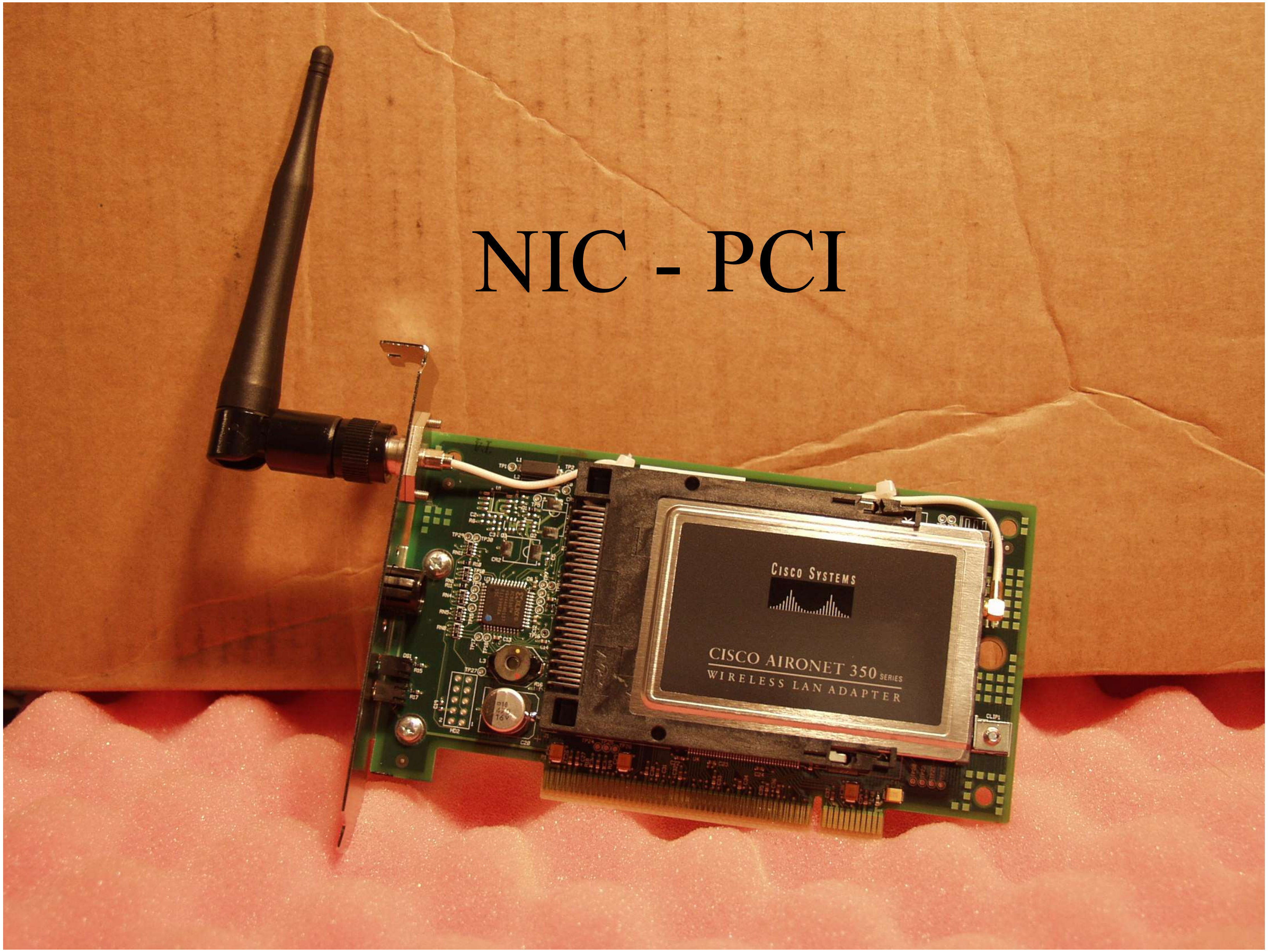
- **AP = Access Point**
  - L2 bridge (802.1d) between wired (802.3) & wireless (802.11)

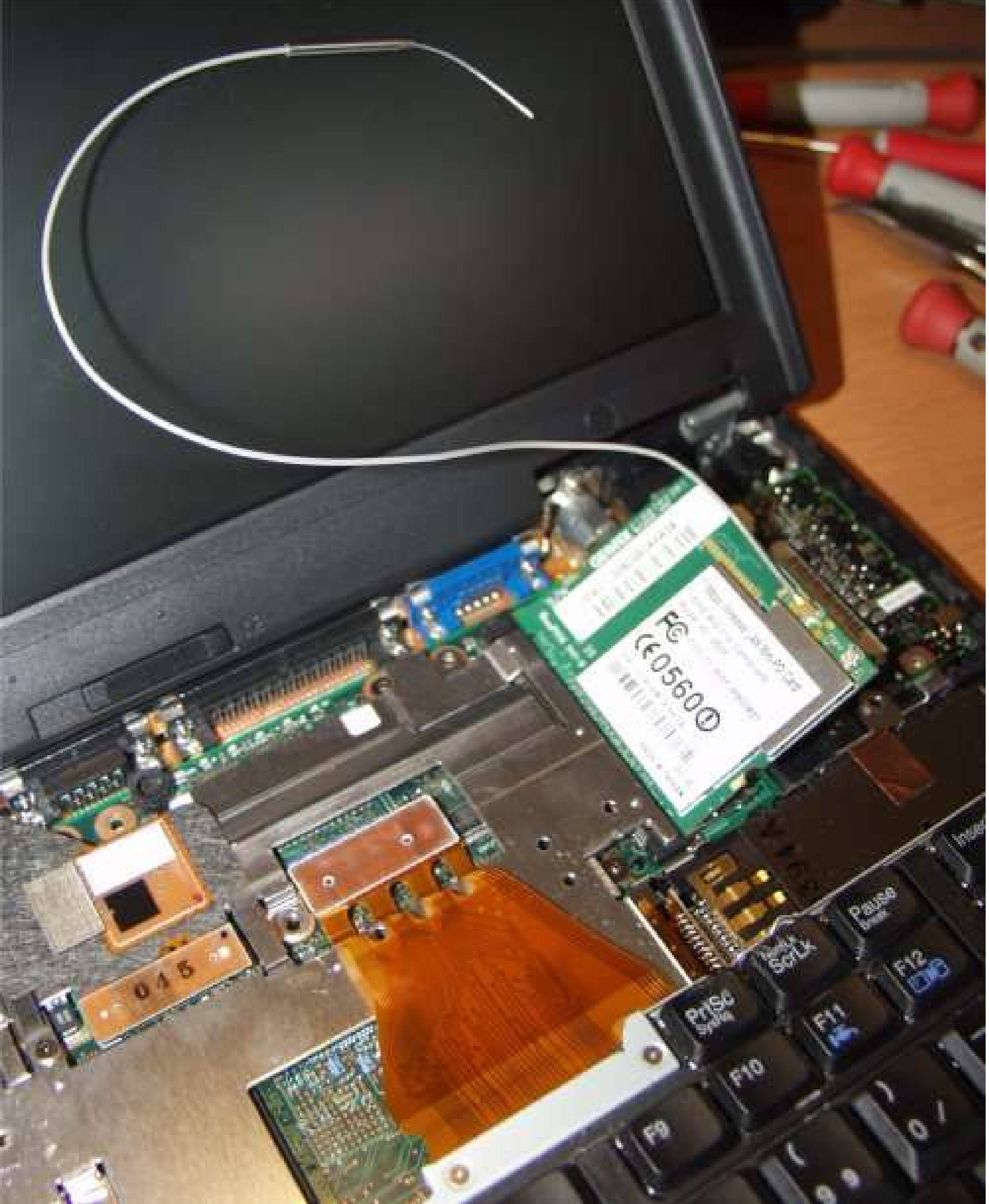
- **STA = Station**
  - 802.11 NIC (PHY in form of PC Card, USB, PCI, etc.)

# NIC – PCMCIA (16) & PC Card (32)



# NIC - PCI

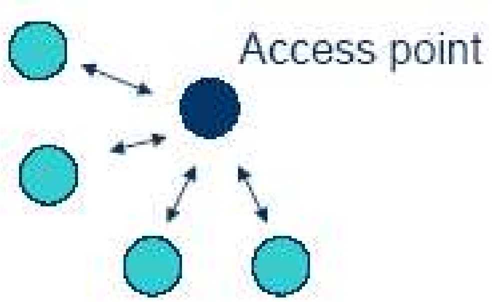

Cisco Systems
CISCO AIRONET 350 SERIES
WIRELESS LAN ADAPTER



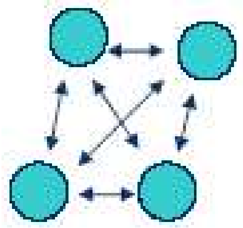
# MiniPCI

# WLAN Modes

- **BSS = Basic Service Set “*Infrastructure*”**
  – L2 bridge between wired (802.3) & wireless (802.11)



- **IBSS = Independent BSS “*Ad-hoc*”**
  – 802.11 NIC (PHY in form of PC Card, USB, PCI, etc.)



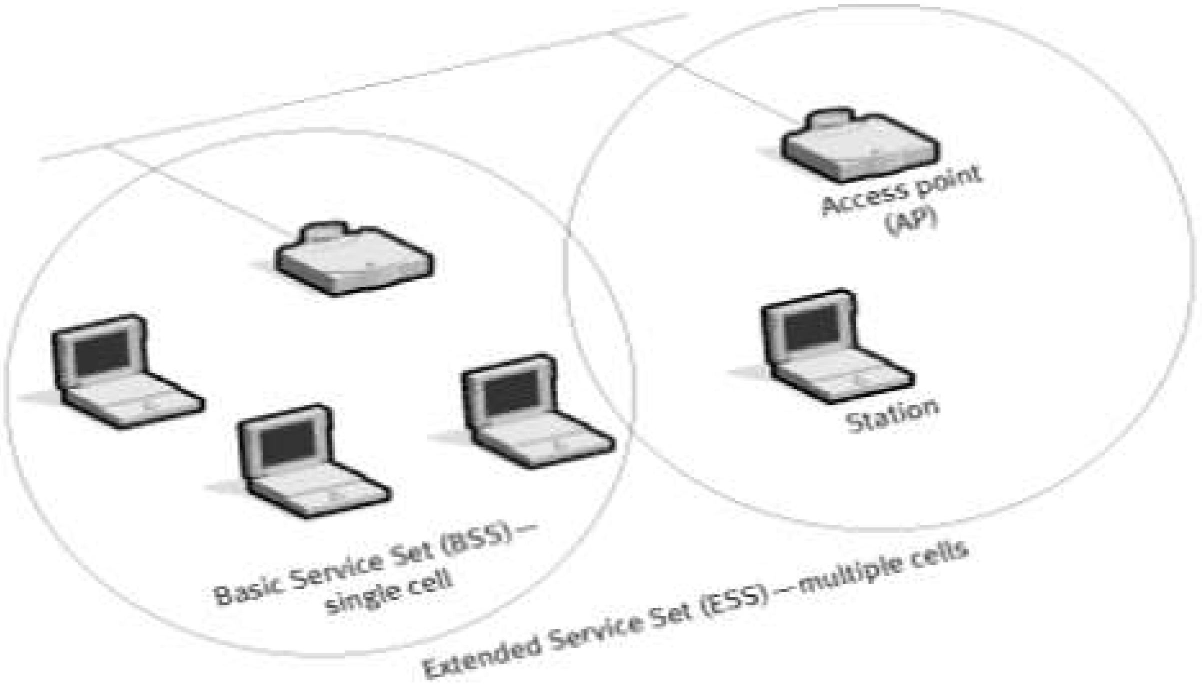
# WLAN Concepts (cont.)

- **SSID = Service Station Identifier**
  - Unique name for network

- **Brief on a the "association" process**
  - AP or IBSS master will "beacon" out an SSID, supported data rates, security requirements, etc. ~10 times a sec
  - STA's send a broadcast "probe" to listen for beacons
  - AP/IBSS master & STA agree on AAA, then sync up
  - STA DHCP's, etc.

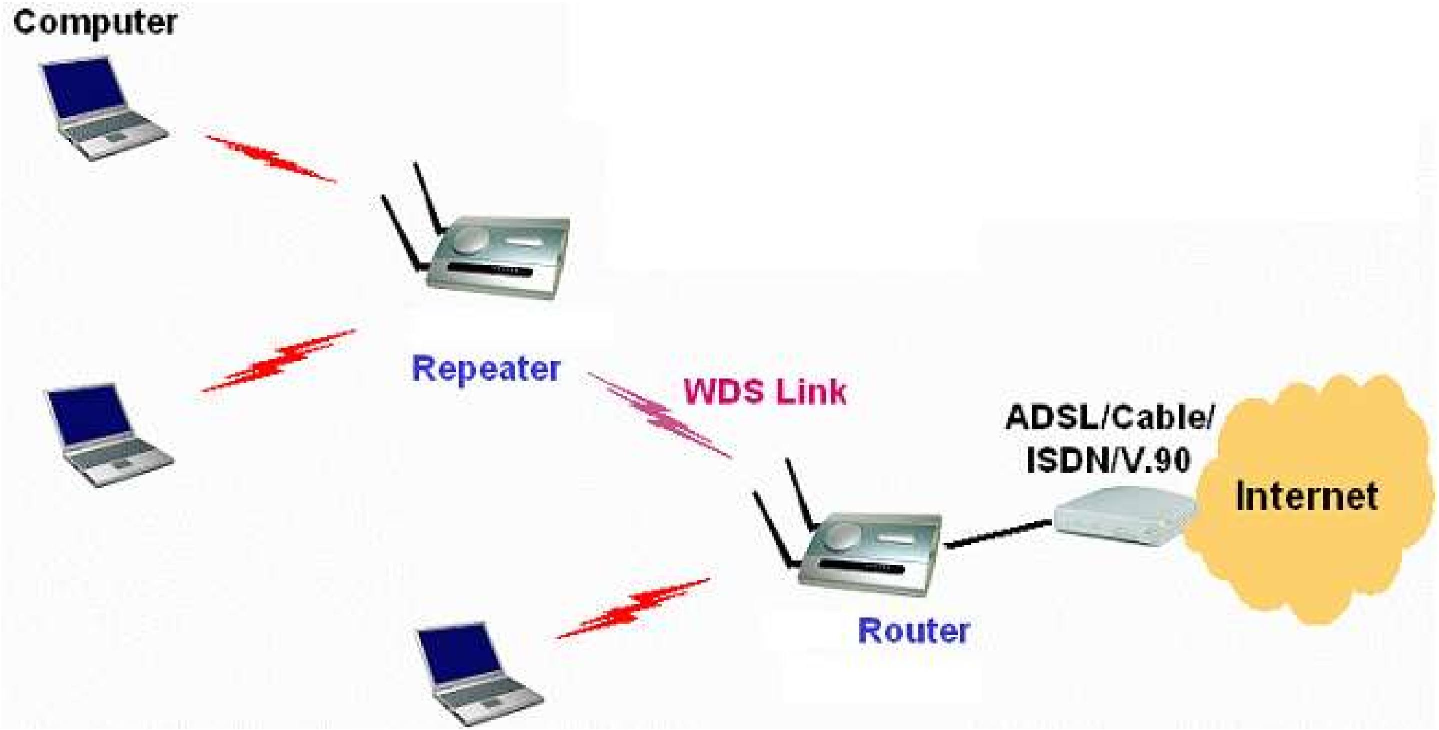
# WLAN Modes (cont.)

- **ESS = Extended Service Set**
  - – Collection of BSS AP's on common backbone

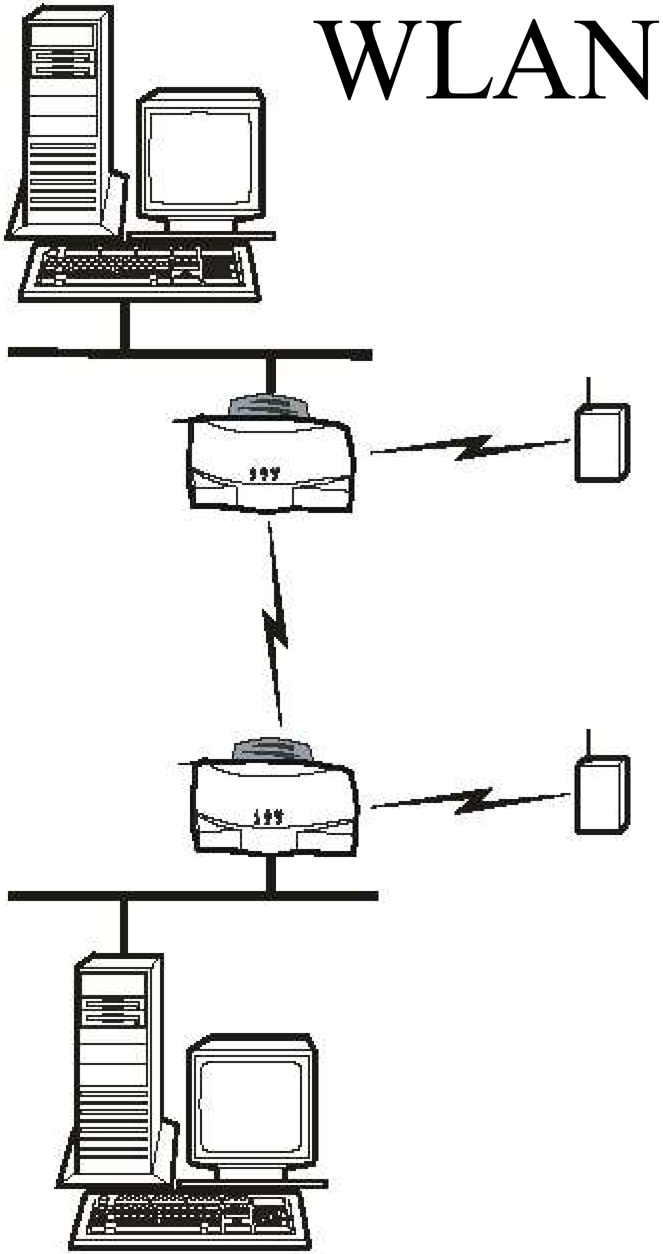


# WLAN Modes (cont.)

- **WDS = Wireless Distribution System**
  - Bridge wired devices over wireless



# WLAN Modes (cont.)



- **WDS & ESS != Mesh**
  - Bridging a wired network wirelessly is NOT 802.11

# AP's : All-in-one

- Products
  - Apple Airport, Linksys WRT54G, etc.

- Standard features
  - Radio (<50mW), DHCP server/client, NAT, HTTP/SNMP management
- Optional features
  - Port filtering, built-in switch, dial-up modem, printer server

# AP's : Enterprise

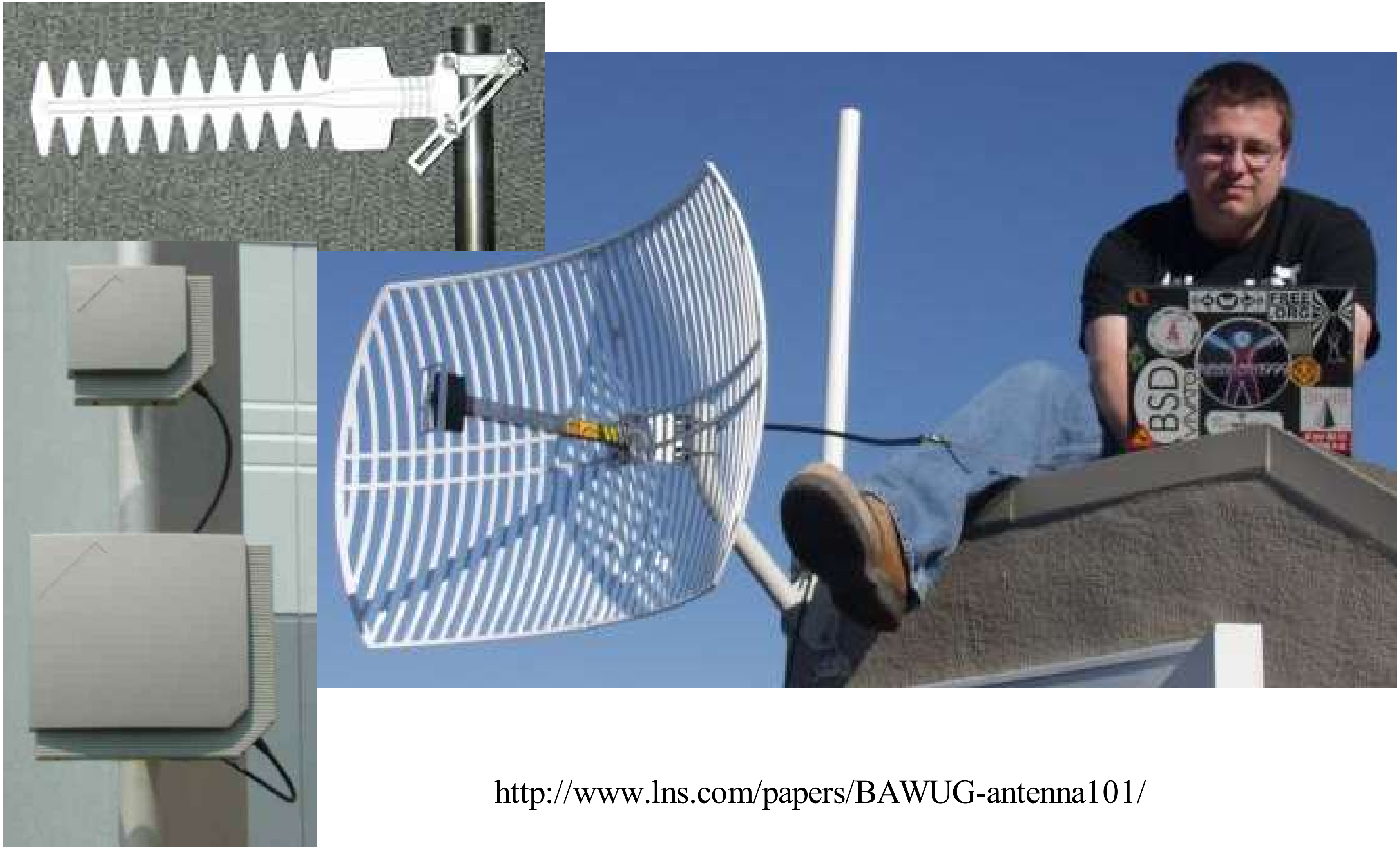
- Products
  - Cisco 1200, Proxim AP-2000, etc.
- Standard features
  - Radio (<100mW), DHCP server/client/relay, HTTP{S}/SNMP/CLI management, antenna ports
- Optional features
  - Port filtering, Power over Ethernet, VLAN tagging, syslog

# AP's : Specialized

- Products
  - Handlink WSG-3000, etc.

- Standard features
  - Radio (<100mW), DHCP server/client/relay, NAT, HTTP{S}/SNMP/CLI management, antenna ports
- Optional features
  - Port filtering, Power over Ethernet, VLAN tagging, syslog, rate limiting, repeater mode

# Antennas

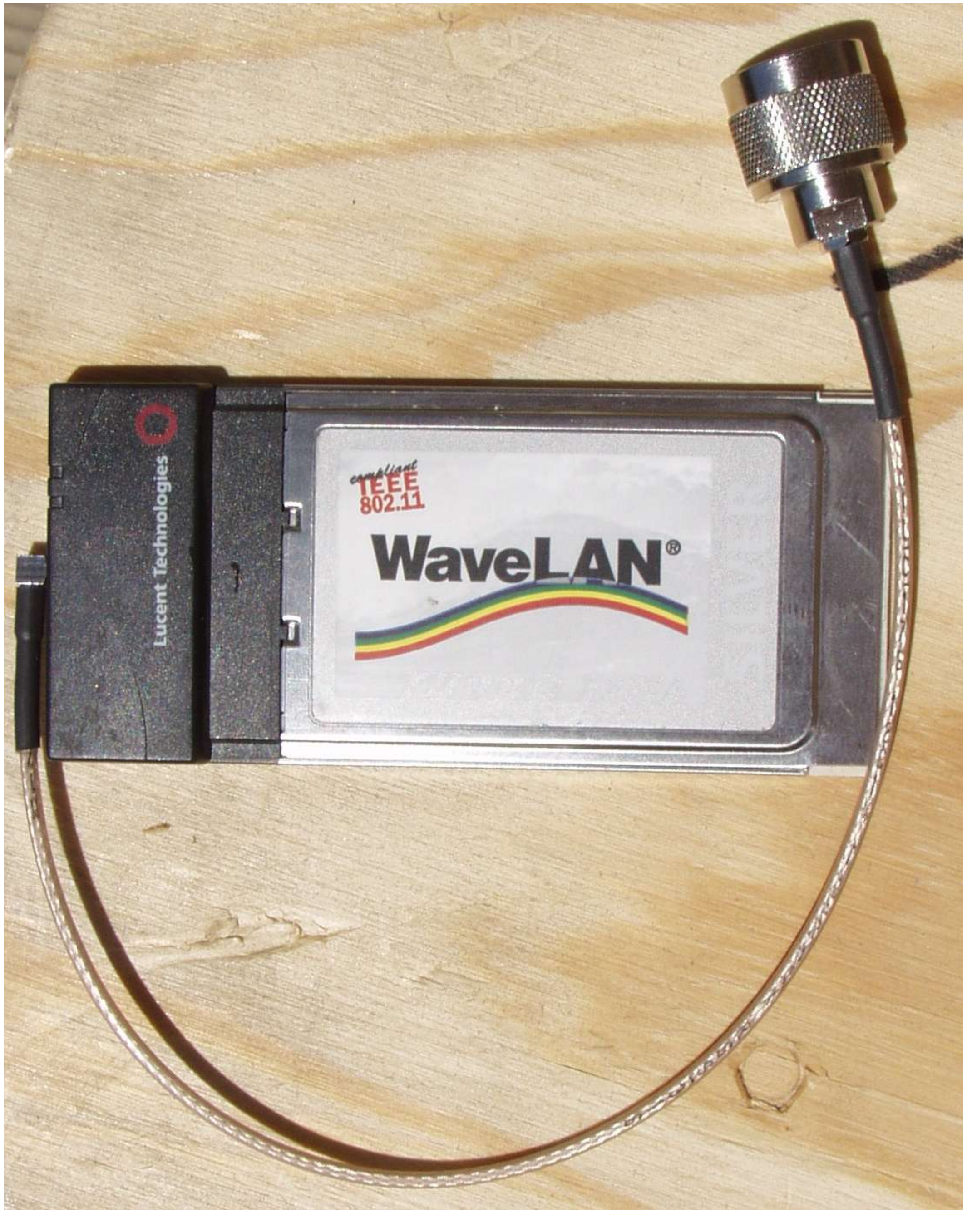


http://www.lns.com/papers/BAWUG-antenna101/

# Antenna Characteristics

- **Polarization**
  - Orientation of element (horiz, vert, circle, etc)
- **Directivity**
  - Size of the beam
- **Bandwidth**
  - Frequencies tuned for
- **Gain**
  - Effective power increase

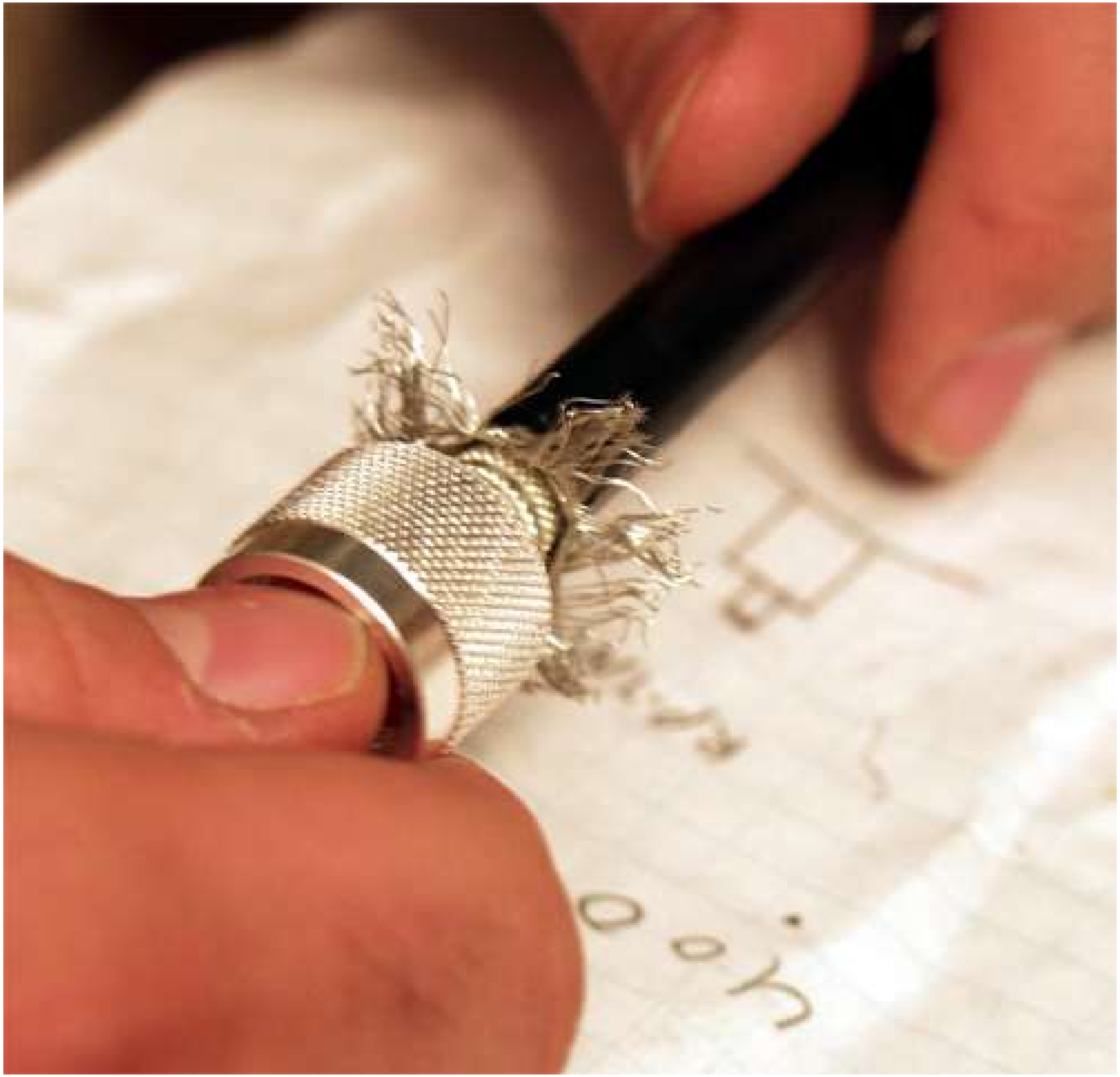
http://www.lns.com/papers/BAWUG-antenna101/



Lucent Technologies
compliant
IEEE
802.11
WaveLAN®

# Making cables..

# Making cables..



# Coax Hints

- Don't use RG-8 (television) cable
  - LMR400 is very popular (low loss/price point)
- Use the correct tools
  - Crimper, soldering iron, heatshrink, glue, etc
- Cheaper (in headache time) to buy pre-made

# Power over Ethernet

- Push DC up unused pairs of Cat5 cable
  - Cost tradeoff
    - No new AC outlets needed
    - Expensive switches or PoE injectors required
  - “Defcon 5” mode
    - Shut em off in a security breach remotly
- Homemade popular, along with IEEE 802.3af

http://www.wi-fiplanet.com/tutorials/print.php/1404631
http://www.nycwireless.net/poe/
http://www.poweroverethernet.com/

Power & Data
Data
Power

# 802.11 Users

- Home/Small Biz
  - $100 Linksys, limited (if any) security
- Enterprise/Academia
  - $1000 AP from Cisco; managed by IT dept., must be secure
- **HSO :** Hotspot Operator
  - Extend wired broadband to wireless-enabled
- **WISP :** Wireless Internet Service Provider
  - Entrepreneur ISP w/o telco broadband infrastructure
- **CWN :** Community Wireless Network)
  - Similar as last two, different “biz model” (more later..)

# WiFi Industries

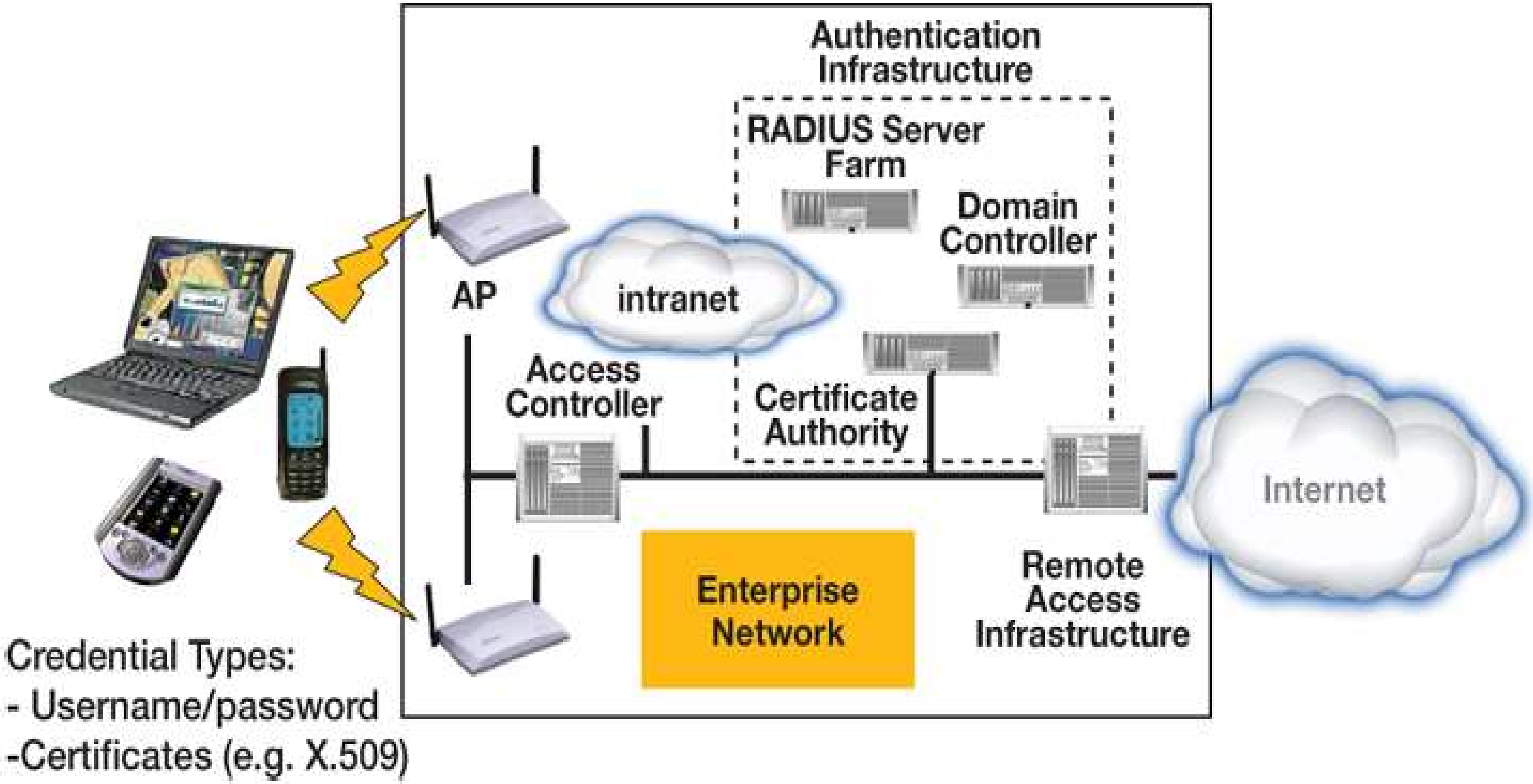
# Hotspot Intro

- Customer is @ Hotel, Airport, Public venue
- Venue/landlord/3rd party provides Internet
  - Wireless, wired or both
  - Backhaul typically XDSL, T1/E1, etc.
- Access is controlled or free
  - Captive portal, WEP key on the wall, etc.
- Market is growing fast
  - 30mil users this year (Gartner), up from 9.3 in 2003

# Hotspot Industry

- **HSO** : Hotspot Operators
  - US : Tmobile, Wayport, Surf and Sip
  - Euro & Asia: BT, Singtel, NTT
- **Aggregators** : think Visa/Plus/Star
  - iPass, Boingo, GRIC, PicoPoint
- **Equipment** : “hotspot in a box”
  - Nomadix, Colubris, NetNearU, Handlink
- **Equipment + Backend**
  - AirPath, Pronto Networks, etc.

# Hotspot Diagram



**Intel : WLAN End to End Guidelines for Enterprise & Hotspot Service Providers**
http://www.intel.com/business/bss/infrastructure/wireless/deployment/e2e_wlan.pdf

# SURF AND SIP™ NETWORK Observations

- 80% of users stay @ same venue
- Can't own the air – SnS covers 5+ Starbucks (Tmobile, diff SSID/channel), competitors cover “our space” too
- Affordable deployment is key!
  - Tmobile typical install $3000 USD (gear only)
  - Surf and Sip $800 USD (inclusive of gear & labor)
- Only “fluff” being VC funded
  - No one funds the people on the “ground floor”

# Hotspot Challenges

- **AAA**
  - 802.1x isn't mainstream (EAP debate continues, PEAP likely to “win” for industry)
  - Many devices aren't HTTPS friendly (PDA's, VoIP, etc)
- **Security**
  - Difficult to provide with a pre-requisite (software)
  - IPsec/SSH/end-to-end recommend

# Hotspot Challenges

- **Roaming**
  - No one wants a dozen accounts!
  - Powerplay between co-op's (WISPr, Pass-One) and 3rd "we'll handle it" parties (iPass, Boingo)
  - Situation has improved; most roam with iPass (int) and Boingo (US)
- **Free vs. Fee**
  - Buy our own Coke machine or use theirs
  - Buy bottled water or slurp from fountain
- **Critical Mass = already?**

# Wireless Internet Service Provider

- **Broadband to the people!**
  - **Where xDSL/cable/etc exists or doesn't exist**
  - **Anywhere from a few m to many km**

http://www.part-15.org/
http://www.wcai.com/

# WISP Outdoor AP's

# WISP Software

- Karlnet
  - – Overcome 802.11 timing issues
- Microtik or StarOS (both Linux based)
  - – RADIUS, DHCP, WDS, Hotspot mode
- Pebble (Linux) or m0n0wall (FreeBSD)
  - – Homegrown solutions, ~easy hacking

# WISP : Customer Antennas

© 02/2004 Matt Peterson

# Site Surveys

- **Should** be a requirement for all deployments
  - The more “paperwork” & planning = more reliable

Calculate path

Visual & RF inspection

Test link

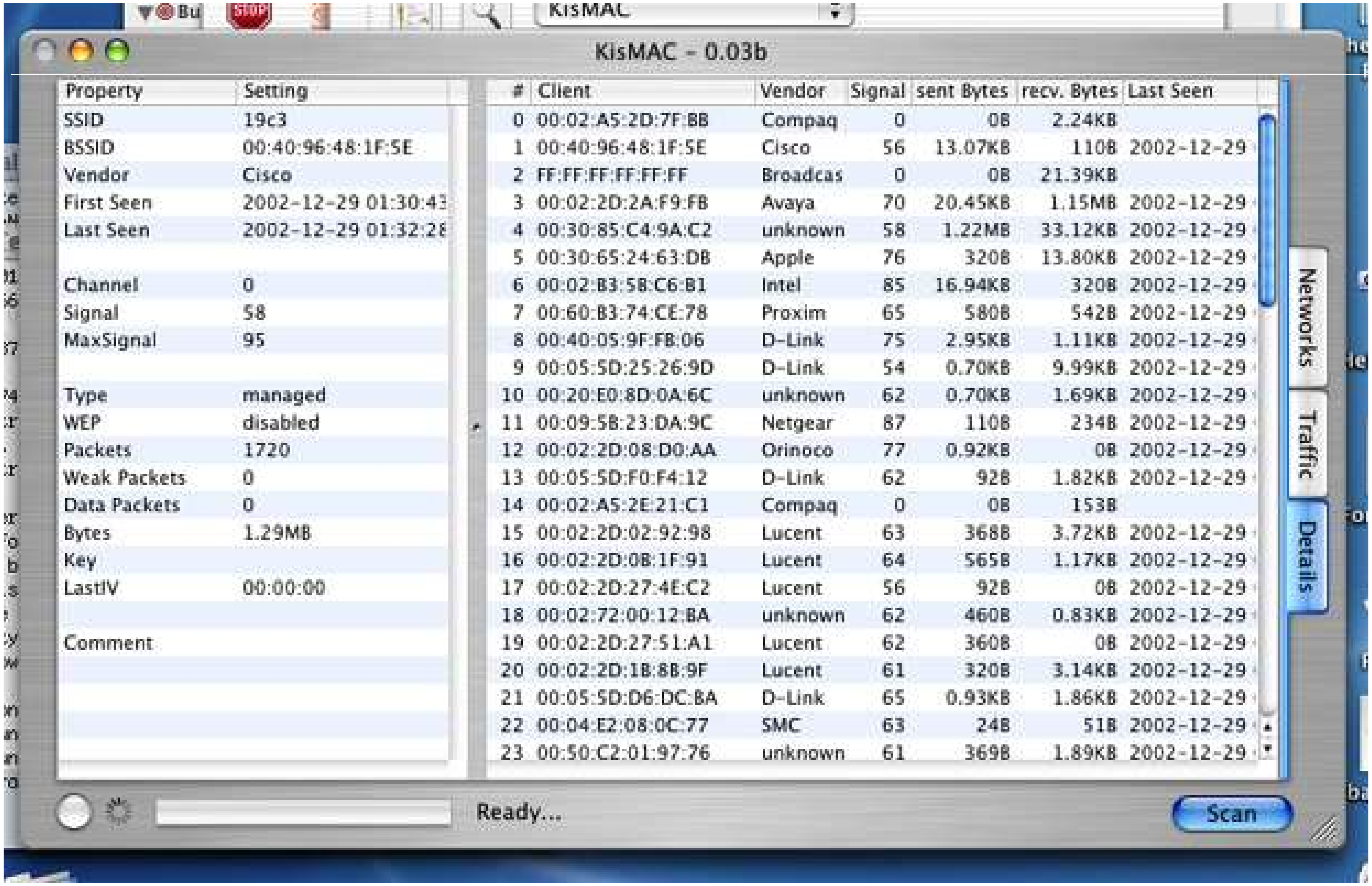
# Site Surveys – Calculate

- Calculate fade margin
  - Input radio output power
  - Loss of coax
  - Gain (power) of antenna
- Tools
  - Free
    - PathCalc (Perl or Excel) http://lns.com/papers/pathcalc/
    - RadioMobile http://cplus.org/rmw/rme.html
  - Commercial $$$
    - EDS, PathLoss, etc.

# Site Surveys - Inspection

- Visual "*Line of Site*"
  - Binoculars, zoomed camera, telescope
  - "Stitch" a 360º panorama of photos http://panoramafactory.com/
  - Note possible objects in path (buildings, antennas, etc.)
- Sniff out interference/competition/neighbors
  - 802.11 "stumbling" (Netstumber, Kismet, etc)
  - Spectrum analyzer will show non-802.11 noise
    - X10 "spy" cameras, cordless phones, HAM's, etc.

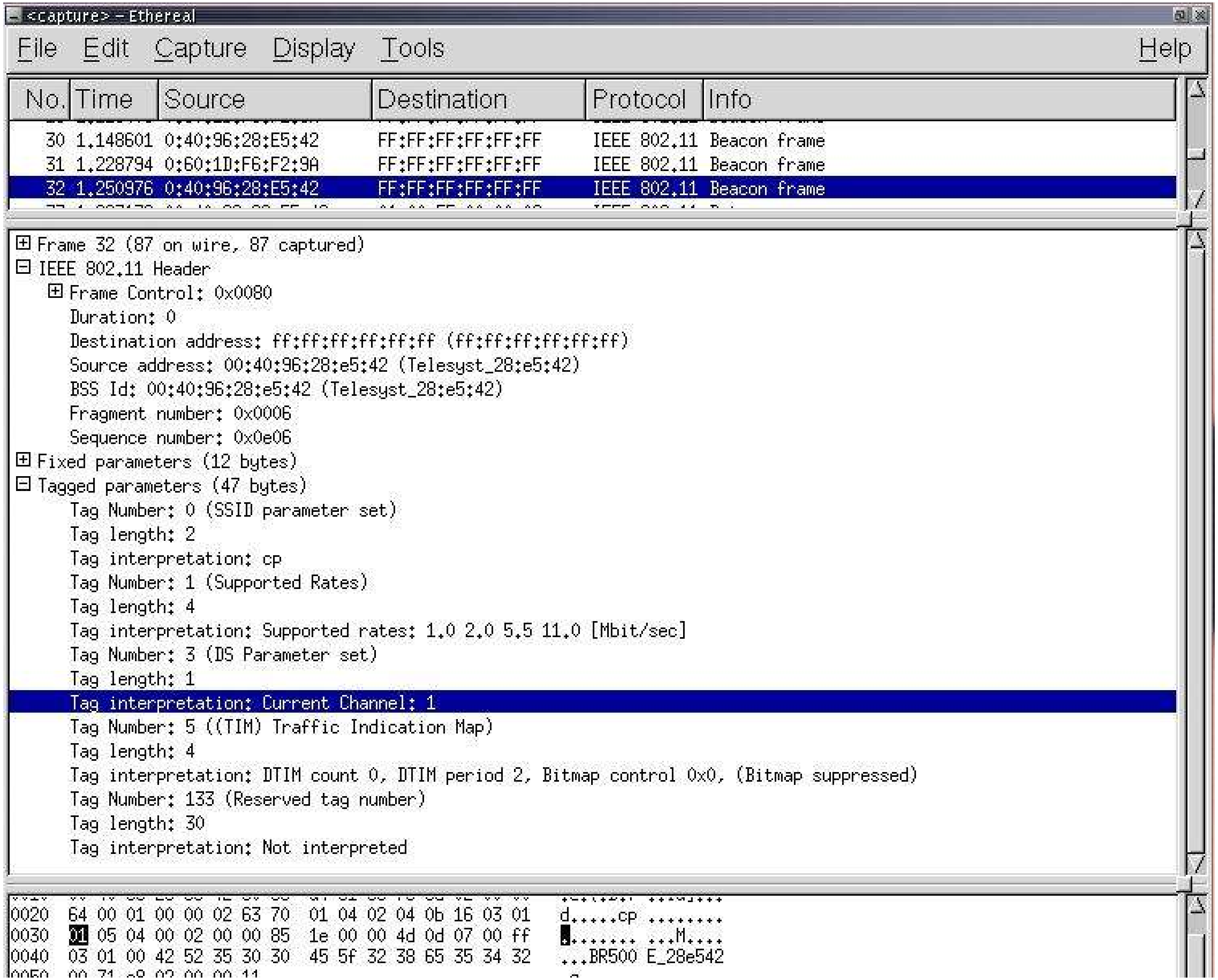
# KisMAC – OS X “Stumbler”



| Property | Setting |
|---|---|
| SSID | 19c3 |
| BSSID | 00:40:96:48:1F:5E |
| Vendor | Cisco |
| First Seen | 2002-12-29 01:30:43 |
| Last Seen | 2002-12-29 01:32:28 |
| | |
| Channel | 0 |
| Signal | 58 |
| MaxSignal | 95 |
| | |
| Type | managed |
| WEP | disabled |
| Packets | 1720 |
| Weak Packets | 0 |
| Data Packets | 0 |
| Bytes | 1.29MB |
| Key | |
| LastIV | 00:00:00 |
| | |
| Comment | |

| # | Client | Vendor | Signal | sent Bytes | recv. Bytes | Last Seen |
|---|---|---|---|---|---|---|
| 0 | 00:02:A5:2D:7F:BB | Compaq | 0 | 0B | 2.24KB | |
| 1 | 00:40:96:48:1F:5E | Cisco | 56 | 13.07KB | 110B | 2002-12-29 |
| 2 | FF:FF:FF:FF:FF:FF | Broadcas | 0 | 0B | 21.39KB | |
| 3 | 00:02:2D:2A:F9:FB | Avaya | 70 | 20.45KB | 1.15MB | 2002-12-29 |
| 4 | 00:30:85:C4:9A:C2 | unknown | 58 | 1.22MB | 33.12KB | 2002-12-29 |
| 5 | 00:30:65:24:63:DB | Apple | 76 | 320B | 13.80KB | 2002-12-29 |
| 6 | 00:02:B3:58:C6:B1 | Intel | 85 | 16.94KB | 320B | 2002-12-29 |
| 7 | 00:60:B3:74:CE:78 | Proxim | 65 | 580B | 542B | 2002-12-29 |
| 8 | 00:40:05:9F:FB:06 | D-Link | 75 | 2.95KB | 1.11KB | 2002-12-29 |
| 9 | 00:05:5D:25:26:9D | D-Link | 54 | 0.70KB | 9.99KB | 2002-12-29 |
| 10 | 00:20:E0:8D:0A:6C | unknown | 62 | 0.70KB | 1.69KB | 2002-12-29 |
| 11 | 00:09:5B:23:DA:9C | Netgear | 87 | 110B | 234B | 2002-12-29 |
| 12 | 00:02:2D:08:D0:AA | Orinoco | 77 | 0.92KB | 0B | 2002-12-29 |
| 13 | 00:05:5D:F0:F4:12 | D-Link | 62 | 92B | 1.82KB | 2002-12-29 |
| 14 | 00:02:A5:2E:21:C1 | Compaq | 0 | 0B | 153B | |
| 15 | 00:02:2D:02:92:98 | Lucent | 63 | 368B | 3.72KB | 2002-12-29 |
| 16 | 00:02:2D:08:1F:91 | Lucent | 64 | 565B | 1.17KB | 2002-12-29 |
| 17 | 00:02:2D:27:4E:C2 | Lucent | 56 | 92B | 0B | 2002-12-29 |
| 18 | 00:02:72:00:12:BA | unknown | 62 | 460B | 0.83KB | 2002-12-29 |
| 19 | 00:02:2D:27:51:A1 | Lucent | 62 | 360B | 0B | 2002-12-29 |
| 20 | 00:02:2D:1B:8B:9F | Lucent | 61 | 320B | 3.14KB | 2002-12-29 |
| 21 | 00:05:5D:D6:DC:BA | D-Link | 65 | 0.93KB | 1.86KB | 2002-12-29 |
| 22 | 00:04:E2:08:0C:77 | SMC | 63 | 24B | 51B | 2002-12-29 |
| 23 | 00:50:C2:01:97:76 | unknown | 61 | 369B | 1.89KB | 2002-12-29 |

# Ethereal - FreeBSD



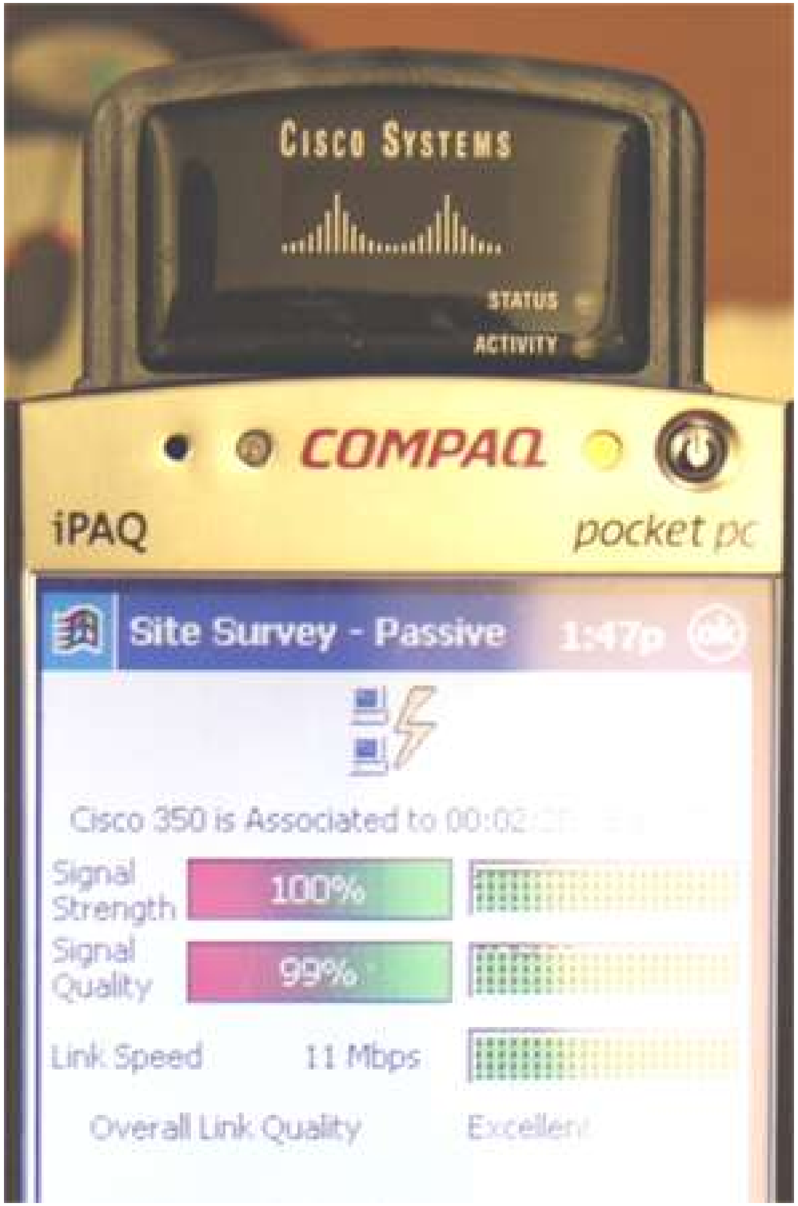
```
No. Time     Source            Destination        Protocol     Info
 30 1.148601 0:40:96:28:E5:42  FF:FF:FF:FF:FF:FF  IEEE 802.11  Beacon frame
 31 1.228794 0:60:1D:F6:F2:9A  FF:FF:FF:FF:FF:FF  IEEE 802.11  Beacon frame
 32 1.250976 0:40:96:28:E5:42  FF:FF:FF:FF:FF:FF  IEEE 802.11  Beacon frame
```

```
⊞ Frame 32 (87 on wire, 87 captured)
⊟ IEEE 802.11 Header
   ⊞ Frame Control: 0x0080
     Duration: 0
     Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
     Source address: 00:40:96:28:e5:42 (Telesyst_28:e5:42)
     BSS Id: 00:40:96:28:e5:42 (Telesyst_28:e5:42)
     Fragment number: 0x0006
     Sequence number: 0x0e06
⊞ Fixed parameters (12 bytes)
⊟ Tagged parameters (47 bytes)
     Tag Number: 0 (SSID parameter set)
     Tag length: 2
     Tag interpretation: cp
     Tag Number: 1 (Supported Rates)
     Tag length: 4
     Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 [Mbit/sec]
     Tag Number: 3 (DS Parameter set)
     Tag length: 1
     Tag interpretation: Current Channel: 1
     Tag Number: 5 ((TIM) Traffic Indication Map)
     Tag length: 4
     Tag interpretation: DTIM count 0, DTIM period 2, Bitmap control 0x0, (Bitmap suppressed)
     Tag Number: 133 (Reserved tag number)
     Tag length: 30
     Tag interpretation: Not interpreted
```

```
0020  64 00 01 00 00 02 63 70  01 04 02 04 0b 16 03 01   d.....cp ........
0030  01 05 04 00 02 00 00 85  1e 00 00 4d 0d 07 00 ff   ........ ...M....
0040  03 01 00 42 52 35 30 30  45 5f 32 38 65 35 34 32   ...BR500 E_28e542
```

© 02/2004 Matt Peterson

# PocketPC PDA



Site Survey - Passive 1:47p ok

Cisco 350 is Associated to 00:02:

Signal Strength 100%

Signal Quality 99%

Link Speed 11 Mbps

Overall Link Quality Excellent

# Site Surveys – Test link

- Cross fingers
  - 100mW NIC + 24dBi grid antenna
  - Note SnR (signal to noise ratio)
- Antennas should be as directional (focused) as possible!

# Security

- Bad things happen
  - Not on purpose, “ANY” STA stumbles on your AP
  - On purpose, “drive-by spam relaying” (spam police knock on your door!)
- Out of the box (all can be defeated)
  - Disable SSID name in beacons
  - MAC address “whitelist” filtering
  - Static WEP keys

# Security (cont.)

- Keep AP firmware updated
- Disable/filter SNMP/CLI/HTTP management
- Note BSSID (MAC address of AP)
  - Rogue AP might have same SSID & channel
  - Again, this too can be spoofed
- Swap out omni antennas to directional
  - Not much security help, but be a nice RF neighbor
- Difficult to shield from RF DoS attacks

# Security (cont.)

- 802.1x AAA + Dynamic WEP keys
  - Who is the user “matt”
  - Is he still employed “yes”
  - What is he allowed access to “IT vlan”
  - Thumps up “here's a personalized WEP key for him”
- Use IPsec or some end-to-end security

**ISS's WLAN FAQ -** http://www.iss.net/wireless/WLAN_FAQ.php

**Strong WEP keys -** http://www.kingsley-hughes.com/tech/security/wep.htm

**Lisa Phifer's Wireless CORner -** http://www.corecom.com/html/wlan.html

# CWN’s : Why?

- **Q:** If we’re both SIP-enabled (ie: MS NetMeeting) and live blocks away from each other, why should our packets go downtown (or across the border) and back?
- **A:** Build an intelligent city/community network; fastest deployment to this nirvana = unlicensed wireless
- CWN’s aren’t limited to wireless; however, digging up the street (fiber) is more difficult then convincing grandma to sponsor an AP on her chimney, etc.
- Geeks have pre-commercial Internet mindset:
  - Symmetrical bandwidth (no **A**DSL, spawn content producers)
  - Real IP v4/v6 space (NAT evil)
  - Limited “legal fluff”, AUP’s

# CWN's : Why?

- If xDSL wasn't popular, many of us CWN's (free) would have been WISP's (fee)
- Extending monopoly infrastructure doesn't led to innovation (commercial hotspot)
- Applications will spawn from networks *without* legacy rules, ethics, other "baggage"
  - Hint : Most WiFi innovation isn't from VC-funded companies (minus Vivato and a few select hardware companies, everything else can be replicated with Linux in weeks)
- We (hundreds of worldwide groups) are begging for a $100 open source box, everyone wants this!

# Community Wireless Networks

- BAWUG - education, spin-off's (SFlan, SFwireless, ThirdBreak, etc)
- NYCwireless, AustinWireless – public hotspots (ie: downtown parks)
- SeattleWireless, BARWN – cityway MAN (ie: Ricochet-like)
- PersonalTelco, NoCatNet – hybrid of above, in-depth web site

# Future

- Unique business models
  - Vendor neutral plays – Airport, Transit
  - Bundled WiFi + …
- “Smart antennas” turned
  - Combo of AP and/or STA “steering” antenna
- IEEE 802.16/WiMAX
  - If the price point is right
- Facts
  - By 2007, 50mil homes will have WiFi (Source: IDC)
  - US only has 5mil now

# Resources - Web

- WiFi Networking News
  - wifinetnews.com
- Hotspot listings
  - jiwire.com
- Broadband Wireless Exchange
  - bbwexchange.com

# Resources - Books

- Wireless Networking Starting Kit
- O'Reilly
  - Wireless Hacks
  - Building Wireless Community Networks
  - 802.11 Wireless Networks : The Definitive Guide
- Real 802.11 Security

ISBN #'s @ http://www.wifinetnews.com/archives/000987.html

# Thanks for this opportunity!

BAWUG

Matt Peterson

matt@bawug.org